5. (Amended) The optical disk according to claim 1, characterised in that said disk further comprises a balancing means for balancing said disk.

6. (Amended) The optical disk according to claim 1, characterised in that the data exchange means is fitted with contacts.

7. (Amended) The optical disk according to claim 1, characterised in that the data exchange means is fitted with a means for transmitting an energy field.

8. (Amended) A method for reading a data storage optical disk comprising the following stages:

an application stage in which data of said disk are applied to a cryptoprocessor via a data exchange means;

a decryption stage in which the cryptoprocessor decrypts the data of said disk from a key; and

an extraction stage in which the decrypted data of the cryptoprocessor are read via a data exchange means;

wherein the optical disk comprises a decryption module, said module comprising a memory including at least one key, a cryptoprocessor, and a data exchange means.

9. (Amended) The method according to claim 8, further comprising an additional stage according to which:

prior to the decryption stage, the data is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface included in an optical disk reader.

10. (Amended) The method according to claim 8, further comprising an additional stage according to which:

prior to the decryption stage, the data is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocerssor interface included in a computer.

11. (Amended) The method according to claim 8, characterised in that in the decryption stage the data is systematically decrypted, whether said data is encrypted or not.

12. (Amended) The method according to claim 8, further comprising an additional stage according to which:

a set of unprocessed data and a set of decrypted data are loaded into a computer, both sets of data originating from a set of data read in the disk.

13. (Amended) The method according to claim 12, characterised in that loading is made alternately.

14. (Amended) The method according to claim 12, characterised in that a set of unprocessed data comprises a zone of unusable encrypted data, and a set of decrypted data comprises a zone of usable decrypted data.

15. (Amended) The method according to claim 12, characterised in that a set of unprocessed data comprises a zone of usable-non-encrypted data, and a set of decrypted data comprises a zone of unusable decrypted data.

16. (Amended) The method according to claim 14, further comprising an additional stage according to which:

an executable code portion in a useful data zone including application data is executed.

17. (Amended) The method according to claim 16, further comprising an additional stage according to which:

various data zones are interconnected, new data is loaded into the memory and a data zone is reconstituted with the aid of a set of links included in the executable code.

18. (Amended) A disk reader device placed to read an optical data storage disk, said device including an interface for exchanging data with a decryption module, wherein the decryption module comprises a memory including at least one secret key, a cryptoprocessor to decrypt the data of said disk from said key, and a data exchange means for applying the data of said disk to the cryptoprocessor and reading the decrypted data of the cryptoprocessor.

19. (Amended) A method for protecting an optical data storage disk comprising:

an encryption stage in which data is encrypted from at least one sole secret key so as to obtain encrypted data;

a writing stage in which the encrypted data are written in said optical disk; and

a loading stage in which the at least one key is loaded into a memory of a decryption module;

wherein said optical data storage disk comprises a decryption module comprising a memory, a cryptoprocessor, and a data exchange means.

20. (Amended) A method for protecting an optical disk for storing data, comprising:

decrypting data of said disk with the aid of a secret key included in a memory of a portable object integrated in said disk and remaining inside said object during decryption,

exchanging the data of said disk between said portable object and said disk by means of data exchange means integrated in said disk.

21. (Amended) The method according to claim 20, characterised in that said portable object comprises a chip with an integrated circuit.

22. (Amended) The method according to claim 20, characterised in that the decryption stage is carried out using a cryptoprocessor integrated in said portable object.

23. (Amended) The method according to claim 22, further comprising an additional stage according to which

prior to the decryption stage, the data is modified into a format able to be understood by the cryptoprocessor via a cryptoprocessor included in an optical disk reader.

24. (Amended) The method according to claim 22, further comprising an additional stage according to which

prior to the decryption stage, the data is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface included in a computer.

25. (Amended) The method according to claim 20, characterised in that the data is decrypted systematically regardless of whether said data was originally encrypted or not.

26. (Amended) The method according to claim 20, further comprising an additional stage according to which:

a set of unprocessed decrypted data originating from a set of data read in the disk is loaded into a computer.

27. (Amended) The method according to claim 26, characterised in that loading is carried out alternately.

28. (Amended) The method according to claim 26, characterised in that a set of unprocessed data comprises a zone of unusable encrypted data and a set of decrypted data comprises a zone of usable decrypted data.

29. (Amended) The method according to claim 26, characterised in that a set of unprocessed data comprises a non-encrypted useful zone of data, and a set of decrypted data comprises a zone of unusable decrypted data.

30. (Amended) The method according to claim 28, further comprising an additional stage according to which:

one executable code portion included in the useful data zone is executed including application data.

31. (Amended) The method according to claim 30, further comprising an additional stage according to which:

at least two data zones are interconnected, new data is loaded into the memory and a data zone is reconstructed with the aid of a set of links included in the executable code.

32. (Amended) The method according to claim 20, further comprising an additional stage according to which:

data is encrypted by means of a secret key, wherein said encrypted data is written in said disk.

33. (Amended) The method according to claim 20, wherein said data forms at least one application written in a high-level language.

34. (Amended) The method according to claim 33, characterised in that the application is at least partially encrypted.

Please add the following new claims:

35. (New) The method according to claim 15, wherein the method comprises an additional stage comprising executing an executable code portion in a useful data zone including application data.